CLAIMS

What is claimed is:

1. A method for preventing Transmission Control Protocol (TCP) synchronize (SYN) package flood attacks, comprising the steps of:

(1) a firewall having received a TCP SYN connection request package from a client, creating a TCP SYN response package for the client and returning to the client by the firewall as an agent of a server, informing the client not to send data packages by the TCP SYN response package;

(2) detecting whether having received a TCP SYN acknowledgement package from the client, if yes, creating a TCP SYN connection request package for the server and sending to the server by the firewall as an agent of the client, otherwise discarding the TCP SYN connection request package from the client;

(3) having received a TCP SYN response package from the server, creating a TCP SYN acknowledgement package for the server and returning to the server,

at same time, creating a TCP SYN acknowledgement package for the client and sending to the client, and initiating data transmission by the TCP SYN acknowledgement package;

(4) forwarding data packages coming from the client to the server by the firewall as an agent of the client, and forwarding data packages coming from the server to the client by the firewall as an agent of the server.

2. The method according to Claim 1, wherein step 1 further comprising, after having received the TCP SYN connection request package from the client, recording source sequence number and window size of the TCP SYN connection request package from the client;

wherein creating a TCP SYN response package for the client comprising, creating the TCP SYN response package with a source sequence number produced by the firewall, a zero window size, source address being the server address and destination address being the client address;

wherein informing the client not to send data packages comprising, basing on the zero window size.

3. The method according to Claim 1, wherein step 2 further comprising, after having received the TCP SYN acknowledgement package from the client, recording window size of the TCP SYN acknowledgement package from the client;

wherein creating a TCP SYN connection request package for the server comprising, creating the TCP SYN connection request package with source sequence number and window size of the TCP SYN connection request package from the client, source address being the client address and destination address being the server address.

4. The method according to Claim 1, wherein step 3 of further comprising: after having received the TCP SYN response package from the

server, recording source sequence number and window size of the TCP SYN response package from the server;

wherein creating a TCP SYN acknowledgement package for the server comprising, creating the TCP SYN acknowledgement package for the server with window size of the TCP SYN acknowledgement package from the client, destination address being the server address and source address being the client address;

wherein creating a TCP SYN acknowledgement package for the client comprising, creating the TCP SYN acknowledgement package with a non-zero window size, destination address being the client address and source address being the server address;

wherein initiating data transmission comprising, basing on the non-zero window size.

5. The method according to Claim 1, wherein forwarding data packages coming from the client to the server by the firewall as an agent of the client comprising, keeping source sequence number and window size of the data package from the client unchanged, calculating a difference between source sequence number of the TCP SYN response package from the server and source sequence number of the TCP SYN response package for the client, modifying acknowledgement sequence number of the data package from the client by increasing the difference, and then sending the modified data package to the server;

wherein forwarding data packages coming from the server to the client by the firewall as an agent of the server comprising, keeping acknowledgement sequence number and window size of the data package from the server unchanged, calculating a difference between source sequence number of the TCP SYN response package from the server and source sequence number of the TCP SYN response package for the client, modifying source sequence number of the data package from the server by decreasing the difference, and then sending the modified data package to the client.